

Troubleshoot Access Point Disassociation from Controller

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Controller-based APs Registration Process](#)

[Use Case 1](#)

[Use Case 2](#)

[Use Case 3](#)

[Use Case 4](#)

[Related Information](#)

Introduction

This document describes use cases to understand the CAPWAP/LWAPP tunnel breaks between Access Points (APs) and the Wireless LAN Controller (WLC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access Points (APs) and Wireless LAN Controller (WLC) configuration
- Routing and Switching.
- Control and Provisioning of Wireless Access Points (CAPWAP)
- Lightweight Access Point Protocol (LWAPP)

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes use cases to understand the reason for the Control and Provisioning of Wireless Access Points (CAPWAP)/Lightweight Access Point Protocol (LWAPP) tunnel break between Access Points (APs) and the Wireless LAN Controller (WLC).

Controller-based APs Registration Process

The APs go through the mentioned process to register with the controller:

1. CAPWAP discovery message request to WLC from APs.
2. The discovery response message from WLC to APs.
3. APs chooses the WLC to join based on the CAPWAP response received.
4. Join Request sent to WLC from APs.
5. The controller validates the APs and sends the join response.

Logs captured on APs when registered with WLC:

Press RETURN to get started!

Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

<Date & time> %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY

<Date & time> status of voice_diag_test from WLC is false

<Date & time> %SSH-5-ENABLED: SSH 2.0 has been enabled

<Date & time> Logging LWAPP message to 255.255.255.255.

<Date & time> %CDP_PD-4-POWER_OK: 15.4 W power - NEGOTIATED inline power source

<Date & time> %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up

<Date & time> %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up

<Date & time> %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to up

<Date & time> %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 255.255.255.255 started - CLI initiated

<Date & time> %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up

Translating "CISCO-LWAPP-CONTROLLER"...domain server (255.255.255.255)

Translating "CISCO-CAPWAP-CONTROLLER"...domain server (255.255.255.255)

<Date & time> %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: <controller IP> peer_port: 5246

<Date & time> %CAPWAP-5-CHANGED: CAPWAP changed state to

<Date & time> %CAPWAP-5-DTLSREQSUCC: DTLS connection created successfully peer_ip: <controller IP> peer_port: 5246

<Date & time> %CAPWAP-5-SENDJOIN: sending Join Request to <controller IP>

<Date & time> %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN

<Date & time> %CAPWAP-5-CHANGED: CAPWAP changed state to CFG

<Date & time> %LWAPP-3-CLIENTERRORLOG: Operator changed mode for 802.11g. Rebooting.

<Date & time> %LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down

<Date & time> %SYS-5-RELOAD: Reload requested by CAPWAP CLIENT. Reload Reason: Operator changed mode for 802.11g.

<Date & time> %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to down

IOS Bootloader - Starting system.

Use Case 1

1. APs get disassociated from WLC and when verified from the switch, it shows that APs has no IP.

Logs when consoled to the APs:

<Date & time> LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0, changed state to up

<Date & time> %CAPWAP-3-ERRORLOG: Not sending discovery request AP does not have an Ip !!

Solution:

Please work to fix the reachability issues to the IP helper address configured under the VLAN if the DHCP server is located remotely. If the DHCP is configured locally ensure there is no DHCP conflict. Configure static IP on the APs:

Log in to APs and type these commands:

```
capwap ap ip address <ip> <mask>
```

```
capwap ap ip default-gateway <ip>
```

Also, you can specify the controller IP address:

```
capwap ap controller ip address <ip>
```

2. Notice that there are APs with IP addresses, but failure to communicate with the WLC could be a resolution failure to controller IP.

Logs from APs with a problem where Domain Name System (DNS) resolution failed:

<Date & time> %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER.local domain

Not in Bound state.

Solution:

Check internal DNS server reachability, if acceptable, ensure Controller IP addresses pushed via DHCP are reachable.

Break-fix: Configure the controller manually on the APs.

```
"capwap ap {primary-base | secondary-base | tertiary-base}controller-name controller-ip-address"
```

3. You see APs is registered on the controller and you still see no broadcast of the required Service Set Identifier (SSID).

```
(4402-d) >config wlan apgroup interface-mapping add <ap group name> <wlandi> <interfacename>
```

Solution:

Please add the Wireless LAN (WLAN) under the APs group.

Use Case 2

Notice that APs is not seen on the Cisco Discovery Protocol (CDP) neighbor of the switch, and APs connected switch is in an error-disabled state.

Logs captured from the Switch:

```
Dec 9 08:42:35.836 UTC: RSTP(10): sending BPDU out Te3/0/47STP: pak->vlan_id: 10
```

```
Dec 9 08:42:35.836 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable stateSTP: pak->vlan_id: 1
```

```
Dec 9 09:47:32.651 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD
```

```
Dec 9 09:47:33.651 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted
```

```
Dec 9 09:47:53.545 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state
```

```
Dec 9 09:48:10.955 UTC: %ILPOWER-5-DETECT: Interface Te3/0/47: Power Device detected: IEEE PD
```

```
Dec 9 09:48:11.955 UTC: %ILPOWER-5-POWER_GRANTED: Interface Te3/0/47: Power granted
```

```
Dec 9 09:48:32.114 UTC: %PM-4-ERR_DISABLE: bpduguard error detected on Te3/0/47, putting Te3/0/47 in err-disable state
```

Solution:

APs does not send the Bridge Protocol Data Unit (BPDU) guard under any circumstances, this is an issue from the switch side. Move the APs to another free port and replicate the interface configuration along with the necessary Physical checks.

Use Case 3

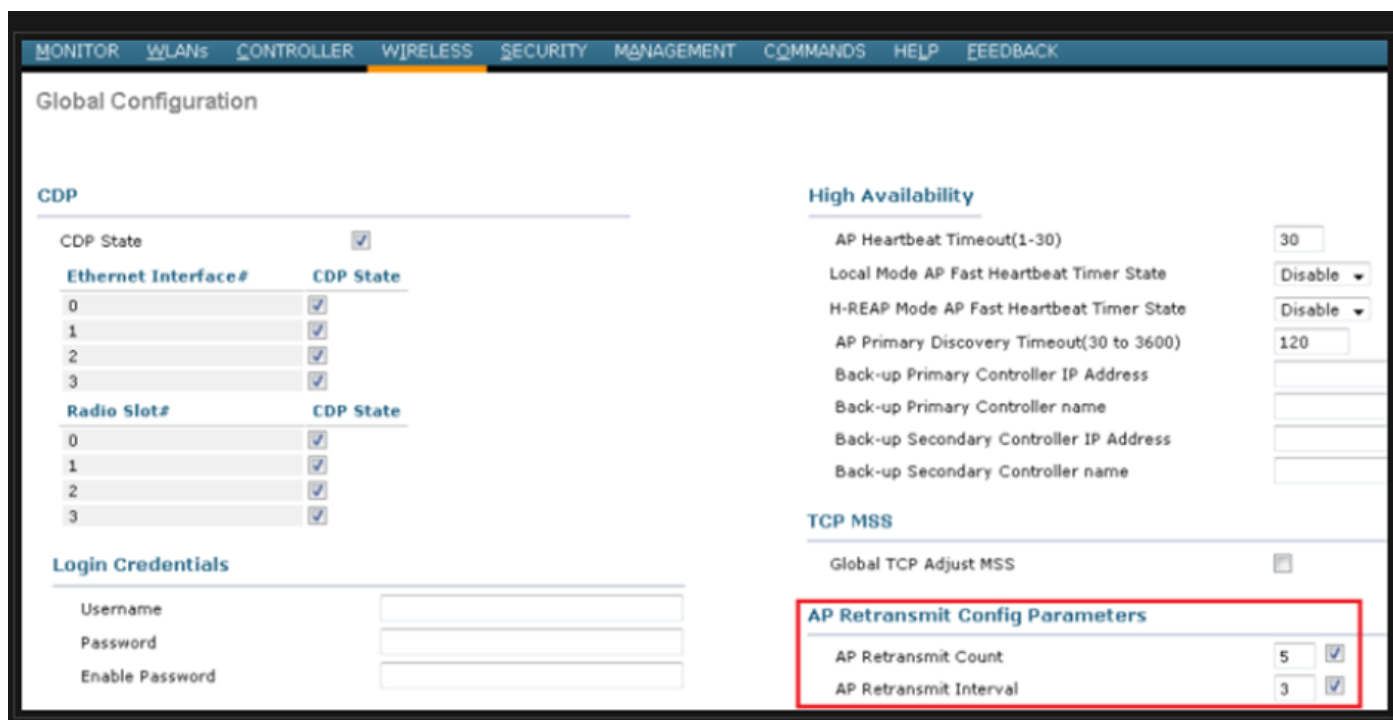
In remote office set-up, you often see CAPWAP tunnel tear down randomly between APs and controller and the most important parameter to check are retransmit and retry interval.

APs retransmit interval and retry interval can be configured both at the global level as well as the APs level. A global configuration applies these configuration parameters to all the APs. That is, the retransmission interval and the retry count is uniform for all APs.

Problematic logs from WLC:

```
*spamApTask6: Jun 01 17:17:55.426: %LWAPP-3-AP_DEL: spam_lrad.c:6088 1c:d1:e0:43:1d:20: Entry deleted for AP: 10.209.36.5 (5256) reason : AP
*spamApTask6: Jun 01 17:17:55.426: %CAPWAP-4-INVALID_STATE_EVENT: capwap_ac_sm.c:9292 The system detects an invalid AP(1c:d1:e0:43:1
-Traceback: 0xe69bba3a5f 0xe69b9b9446 0xe69bdc5e3b 0xe69b8f238c 0xe69bbaf33b 0xe69cc8041b 0xe69c71df97 0x7fef39282dff 0x7fef3869f98d
*spamReceiveTask: Jun 01 17:17:55.426: %CAPWAP-4-INVALID_STATE_EVENT: capwap_ac_sm.c:9292 The system detects an invalid AP(1c:d1:e0:43:1
-Traceback: 0xe69bba3a5f 0xe69b981950 0xe69b76dd5c 0xe69cc757c2 0xe69c71df97 0x7fef39282dff 0x7fef3869f98d
*spamApTask5: Jun 01 17:17:55.424: %CAPWAP-3-DTLS_CLOSED_ERR: capwap_ac_sm.c:7521 1c:d1:e0:43:1d:20: DTLS connection closed forAP
*spamApTask5: Jun 01 17:17:55.423: %CAPWAP-3-MAX_RETRANSMISSIONS_REACHED: capwap_ac_sm.c:8073 Max retransmissions reached on
),number of pending messages(2)
```

Solution: If the issue is across all sites increase the **Retransmit count** and **Retransmit interval** under wireless Global configuration. Option to increase the values when the problem is for all the APs.



The screenshot displays the Cisco Wireless LAN Controller (WLC) Global Configuration page. The page is divided into several sections: CDP, High Availability, TCP MSS, and AP Retransmit Config Parameters. The AP Retransmit Config Parameters section is highlighted with a red box and contains the following settings:

Parameter	Value	Checkbox
AP Retransmit Count	5	<input checked="" type="checkbox"/>
AP Retransmit Interval	3	<input checked="" type="checkbox"/>

Option to change AP retransmit config parameters under Global configuration

If the problem is specific to one remote site, an increase in **Retransmit count** and **Retransmit interval** on a particular APs fixes the issue.



Option to change AP retransmit config parameter under a specific APs

Use Case 4

The APs gets completely disassociated from the WLC and is not able to rejoin the controller this could be related to the digital certificates.

Some quick facts about device certificates in terms of Cisco WLCs and APs:

- Every device that comes out from Cisco comes with a certificate by default with a validity of 10 years.
- This certificate is used to perform authentication between the Cisco WLC and APs.
- With the help of certificates APs and WLC establish a secure Datagram Transport Layer Security (DTLS) tunnel.

Encountered two types of issues related to certificates:

Issue 1: Older APs (does not want to join WLC).

Console to the APs helps determine the problem and logs look as follows:

```
*Sep 13 18:26:24.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.1.1.1 peer_port: 5246
*Sep 13 18:26:24.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Sep 13 18:26:24.099: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed.
The certificate (SN: XXXXXXXXXXXXXXXX) has expired. Validity period ended on 19:56:24 UTC Aug 12 2018
*Sep 13 18:26:24.099: %LWAPP-3-CLIENTERRORLOG: Peer certificate verification failed
*Sep 13 18:26:24.099: %CAPWAP-3-ERRORLOG: Certificate verification failed!
```

Issue 2: Newer APs does not want to join an older WLC.

The console to the APs gives an error that could look like this:

```
[*09/09/2019 04:55:26.3299] CAPWAP State: DTLS Teardown
[*09/09/2019 04:55:30.9385] CAPWAP State: Discovery
[*09/09/2019 04:55:30.9385] Did not get log server settings from DHCP.
[*09/09/2019 04:55:41.0000] CAPWAP State: DTLS Setup
[*09/09/2019 04:55:41.3399] Bad certificate alert received from peer.
```

[*09/09/2019 04:55:41.3399] DTLS: Received packet caused DTLS to close connection

Solution:

1. NTP disables and sets the time manually through CLI:

```
(Cisco Controller)> config time ntp delete 1
```

```
(Cisco Controller)> config time manual 09/30/18 11:30:00
```

2. NTP disables and sets the time manually through GUI:

Navigate to **Controller > NTP > Server > Commands > Set Time** in order to remove the listed NTP servers.

The screenshot shows the Cisco GUI interface for configuring the system time. The top navigation bar includes tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS (selected), and HELP. The left sidebar lists various system commands, with 'Set Time' highlighted. The main content area is titled 'Set Time' and displays the current time as 'Tue Jan 31 17:47:08 2023'. Below this, there are three sections: 'Date', 'Time', and 'Timezone'. The 'Date' section has dropdown menus for Month (January), Day (31), and Year (2023). The 'Time' section has input fields for Hour (17), Minutes (47), and Seconds (8). The 'Timezone' section has input fields for Delta (hours: 0, mins: 0) and a dropdown menu for Location (-Select Location-).

Location to Set time manually on the GUI

2. Disable the Manufacturer Installed Certificate (MIC) on the controller. This command is accepted only on the latest versions.

```
(Cisco Controller)> config ap cert-expiry-ignore mic enable
```

Related Information

- [Cisco Technical Support & Downloads](#)